UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/853,770	05/11/2001	Satoshi Shigematsu	96790P355	6640

8791	7590	03/09/2006	

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER
TRAN, ELLEN C

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 03/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/853,770	SHIGEMATSU ET AL.
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>*11 January 2005*</u>.

2a) ☐ This action is **FINAL.**   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle,* 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-50 and 83-93* is/are pending in the application.

     4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-50 and 83-93* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

     a)☐ All   b)☐ Some * c)☐ None of:

         1. ☒ Certified copies of the priority documents have been received.

         2. ☐ Certified copies of the priority documents have been received in Application No. _____.

         3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

     * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>*5/01-2/06*</u>.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   This action is responsive to communication: filed on 11 January 2005 with an original

application filed 11 May 2001, with acknowledgement of foreign priority data from 12 January

2001. The delay in the office response is because the applicant's response was mistakenly

scanned with submitted IDS.

2.   The 11 January 2005 communication is a response to a restriction, the applicant elected

without traverse Group I, therefore claims 1-50 and 83-93 are currently pending in the

application. Claims 1, 10, 21, 25, 29, 3, 37, and 44 are independent claims. Claims 51-82 are

withdrawn from consideration because they were not elected.

Claim Rejections - 35 USC § 112

3.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and
> distinctly claiming the subject matter which the applicant regards as his invention.

4.   Claims 1-20, and 83-93 are rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention. Independent claims 1 and 10, and several of their dependent

claims contain the following text: "when the user is to use a use device", it is indefinite what the

applicant is trying to convey: "use a use device" is indefinite because the words do not provide a

further limitation. Appropriate correction is required in all occurrences of "use a use device".

Information Disclosure Statement

5.   Some of the information disclosure statements filed from May of 2001 through February

2006 fail to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because no

English translation provided about the content of Japanese Patents and other foreign patents, or

portion identified and translated about the portion of Patents that is relevant. It has been placed

in the application file, but the information referred to therein has not been considered as to the

merits. Applicant is advised that the date of any re-submission of any item of information

contained in this information disclosure statement or the submission of any missing element(s)

will be the date of submission for purposes of determining compliance with the requirements

based on the time of filing the statement, including all certification requirements for statements

under 37 CFR 1.97(e). See MPEP § 609.05(a). The applicant is also advised that some of the

other documents in the information disclosure have been considered such as US Patents or

foreign patents in English; in addition when the translated Japanese Patent Abstract was provided

and noted on the IDS form it was considered.

Claim Rejections - 35 USC § 102

6.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section
> 122(b), by another filed in the United States before the invention by the applicant for
> patent or (2) a patent granted on an application for patent by another filed in the United
> States before the invention by the applicant for patent, except that an international
> application filed under the treaty defined in section 351(a) shall have the effects for
> purposes of this subsection of an application filed in the United States only if the
> international application designated the United States and was published under Article
> 21(2) of such treaty in the English language.

7.   **Claims 37-39 and 44-46** are rejected under 35 U.S.C. 102(e) as being anticipated by

Saito et al. U.S. Patent No. 6,980,672 (hereinafter '672).

As to independent claim 44, "A lock/unlock method for a biometrical information authentication storage which locks or unlocks a door of a main body in storing an article in the main body or taking out the article stored in the main body, and also unlocks the door on the basis of authentication of biometrical information of a user, comprising: the first step of unlocking the door on the basis of matching between stored information stored in storage means in advance and detected information from a sensor for detecting the biometrical information of the user" is taught in '672 col. 2, lines 1-11.

As to dependent claim 45, "wherein the storage means stores a fingerprint image of the user as the biometrics information, and processing in the first step comprises the second step of unlocking the door on the basis of matching between the stored information in the storage means and the fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information" is shown in '672 col. 2, lines 1-11.

As to dependent claim 46, " wherein processing in the second step comprises the third step of, when the fingerprint image of the user, which is transmitted from the fingerprint authentication token, is received in storing the article in the main body, locking the door and storing the received fingerprint image in the storage means" is disclosed in '672 col. 2, lines 48-54;

"and the fourth step of unlocking the door when the fingerprint image of the user, which is transmitted from the fingerprint authentication token, is received in taking out the article stored in the main body, and the received fingerprint image matches the stored information in the storage means" is taught in '672 col. 3, lines 15-39.

As to independent claim 37, this claim is directed to a process for to executing the authentication

procedure of claim 44; therefore it is rejected along similar rationale.

As to dependent claims 38 and 39, these claims contain substantially similar subject matter as claims

45 and 46; therefore they are rejected along similar rationale.

Scott et al

8.   **Claims 1-6, 8, 83-86** are rejected under 35 U.S.C. 102(e) as being anticipated by ~~Saito et~~

6,484,260   ('260)

al. U.S. Patent No. ~~6,980,672 (hereinafter '672).~~

As to independent claim 1, **"An authentication token which is normally held by a user and,**

when the user is to use a use device for executing predetermined processing in accordance

with authentication data of the user, connected to the use device to perform user

authentication on the basis of biometrical information of the user, comprising: a personal

collation unit including a sensor for detecting the biometrical information of the user and

outputting a detection result as sensing data, a storage unit which stores in advance

registered data to be collated with the biometrical information of the user, and a collation

unit for collating the registered data stored in said storage unit with the sensing data

from said sensor and outputting a collation result as authentication data representing a

user authentication result; and a communication unit for transmitting the

authentication data from said personal collation unit to the use device as communication

data, wherein said personal collation unit and communication unit are integrated" is taught

in '260 col. 1, line 46 through col. 2, line 21.

As to dependent claim 2, "wherein said storage unit further stores in advance user information unique to the user, which is to be used for processing in the use device, and said collation unit outputs the authentication data containing the user information read out from said storage unit" is shown in '260 col. 2, lines 15-43.

As to dependent claim 3, "further comprising a protocol conversion unit for converting the communication data from said communication unit into a predetermined data format and transmitting the communication data to the use device" is disclosed in '260 col. 2, lines 22-39.

As to dependent claim 4, "further comprising a radio unit for transmitting the communication data from said communication unit to the use device through a radio section" is taught in '260 col. 7, lines 35-58.

As to dependent claim 5, "further comprising a radio unit for transmitting the communication data from said protocol conversion unit to the use device through a radio section" is shown in '260 col. 7, lines 35-38.

As to dependent claim 6, "further comprising a battery for supplying power" is disclosed in '260 col. 6, lines 29-39.

As to dependent claim 8, "wherein said storage unit has, in addition to a storage area for storing the registered data, at least one storage area for storing another information" is taught in '260 col. 2, lines 27-38.

As to dependent claim 83, "wherein said token further comprises an encryption circuit for encrypting data generated from the authentication data and dynamic information generated by the use device and transmitted using a key registered in advance, and said communication circuit transmits to the use device encrypted data generated by said encryption circuit" is shown in '260 col. 2, lines 22-39.

As to dependent claim 84, "wherein said token further comprises a result determination circuit for, when the collation result indicates that the authentication is successful, outputting the authentication data to said encryption circuit, and when the collation result indicates that the authentication fails, outputting the authentication data to said first communication circuit, and 10 an encryption circuit for, in accordance with the authentication data from said result determination circuit, encrypting dynamic information transmitted from the use device using a key registered in advance, adding obtained encrypted data to the authentication data, and outputting the encrypted data, and said communication circuit transmits to the use device the authentication data with the encrypted data from said encryption circuit or the authentication data from said result determination circuit" is disclosed in '260 col. 2, lines 22-39.

As to dependent claim 85, "wherein said token further comprises an encryption circuit for encrypting dynamic information transmitted from the use device using a key registered in advance and outputting obtained encrypted data to said first communication circuit as data, and a first result determination circuit for, when the collation result indicates that the authentication is successful, instructing said encryption circuit to generate the encrypted data, and when the collation result indicates that the authentication fails, outputting data whose number of digits is different from that of the encrypted data to said first communication

circuit, and said first communication circuit transmits to the use device the data from said

encryption circuit or the data from said first result determination circuit" is shown in '260 col.

3, lines 29-65 (note the "password" is interpreted to have the same meaning as the "random

number").

As to dependent claim 86, "wherein said token further comprises an ID storage circuit for

storing identification information of said authentication token registered in advance, and

said first communication circuit transmits to the use device the identification information

stored in said ID storage circuit" is disclosed in '260 col. 3, lines 23-28.

Claim Rejections - 35 USC § 103

9.　　　The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or
> described as set forth in section 102 of this title, if the differences between the subject matter
> sought to be patented and the prior art are such that the subject matter as a whole would have
> been obvious at the time the invention was made to a person having ordinary skill in the art to
> which said subject matter pertains. Patentability shall not be negatived by the manner in which
> the invention was made.

10.　　　**Claims 9-18, 20-36, and 87-93,** are rejected under 35 U.S.C. 103(a) as being

unpatentable over '260 in further view of Sumino U.S. Patent No. 6,957,338 (hereinafter '338).

As to independent claim 10, "An authentication system for executing user authentication,

which is necessary for use of a use device for executing predetermined processing, by

using biometrical information of a user, comprising: an authentication token which is

normally held by the user and, when the user is to use said use device, connected to said use device

to perform user authentication on the basis of the biometrical information of the user, said

authentication token comprising a personal collation unit including a sensor for detecting

the biometrical information of the user and outputting a detection result as sensing data,

a storage unit which stores in advance registered data to be collated with the biometrical

information of the user, and a collation unit for collating the registered data stored in said

storage unit with the sensing data from said sensor and outputting a collation result

representing a user authentication result as authentication data, and a first communication

unit for transmitting the authentication data from said personal collation unit to said use

device as communication data, said personal collation unit and communication unit being

integrated" is taught in '260 col. 1, line 46 through col. 2, line 21;

the following is not taught in '260: "and said use device comprising a second communication

unit for receiving the communication data transmitted from said authentication token and

outputting the data as the authentication data, and a processing unit for executing the

predetermined processing on the basis of the collation result contained in the authentication

data from said second communication unit" however '338 teaches "a

collatng unit for respectively collating the biological information and

the password output" in col. 1, lines 63-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention

to modify the teachings of '260 a portable personal identification system utilizing biometrics to

include a means to store passwords in the personal devices as taught in '338. One in the art

would have been motivated to perform such a modification because as indicated by '338 a need

exist to combine the authentication cards used that store passwords with biometrics to insure

security (see '338 col. 1, lines 32-51 "However, even in the individual authentication system

using the IC card, if both the IC card (a physical object) and the password (individual

knowledge) are stolen, the safety is not secured ... an object of the present invention is to

provide an individual authentication system by which the data processing device which needs

individual authentication can be used and managed with higher security".

As to dependent claim 12, "**wherein said storage unit of said authentication token stores in**

advance user information unique to the user, which is to be used for processing in said use

device, said collation unit of said authentication token outputs the authentication data

containing the user information read out from said storage unit, and said processing unit of

said use device executes processing using the user information contained in the

authentication data from said second communication unit" is taught in '338 col. 1, lines 54-67.

As to dependent claim 9, "**wherein said at least one storage area for storing another**

information includes a storage area for storing personal information of the user and a storage

area for storing service information" is shown in '228 col. 1,

lines 54-67.

As to dependent claims 11, 13-18, 20, and 87-93 these claims contain substantially similar subject matter as claims 3-9

and 83-86 above, therefore they are rejected along similar rationale.

As to independent claim 25, "**An authentication method of executing user**

authentication, which is necessary when a user is to use a service providing apparatus for

providing a predetermined service, between the service providing apparatus and provides

the service to the user on the basis of a collation result and an authentication token for

executing the user authentication using biometrical information of the user, wherein" is

taught in '260 col. 1, line 46 through col. 2, line 21;

"the authentication token stores in advance a password of the authentication token

and token identification information for identifying the authentication token, performs

collation on the basis of the biometrical information detected from the user to check whether

the user is an authentic user and when a collation result indicates that collation is successful,

transmits the password and token identification information to the service providing

apparatus as communication data, and authentication token in advance in a first database in

association with each other, collates the password contained in the communication data

received from the authentication token with a password obtained from the first database

using the token identification information as a key" is shown in '338 col. 1, lines 54-67 "an

individual authentication card for storing biological information and a password for identifying a

registered user" (registered is interpreted to mean the information was provided in advance).

As to dependent claim 26, "wherein the token identification information and password are

registered in the first database in association with each other from a registration apparatus

connected to the service providing apparatus through a communication network" is disclosed in

'260 col. 5, lines 55-58 "The personal identification device can be used in conjunction with conventional

telephone lines or computer network communications".

As to dependent claim 27, "wherein the service providing apparatus causes a password

generation circuit to generate a new password, transmits the new password to the

authentication token through the second communication unit, and updates the password

stored in the first database, and the authentication token updates the password stored in

advance by the new password received from the service providing apparatus" is taught in '260

col. 3, lines 29-67 (note the generated random number is interpreted to have the same meaning as

the new password).

As to dependent claim 28, "wherein the service providing apparatus stores device identification

information for identifying the service providing apparatus in advance, and transmits the

device identification information to the authentication token when the authentication token

is connected, and the authentication token stores in advance the password and the device

identification information for identifying the service providing apparatus in a second

database in association with each other, and uses, as the password to be transmitted to the

service providing apparatus, a password obtained from the second database using the device

identification information received from the service providing apparatus as a key" is

shown in '260 col. 3, lines 29-67.

As to independent claim 29, this claim is directed to a recording medium for causing a computer to

execute the authentication procedure of claim 25; therefore it is rejected along similar rationale.

As to dependent claims 30-32, these claims contain substantially similar subject matter as claims 26-

28; therefore they are rejected along similar rationale.

As to independent claim 33, this claim is directed to a program for causing a computer to execute the

authentication procedure of claim 25; therefore it is rejected along similar rationale.

As to dependent claims 34-36, these claims contain substantially similar subject matter as claims 26-

28; therefore they are rejected along similar rationale.

As to independent claim 21, this claim contains the limitations previously presented in claims 1, 10, and 25; therefore it is rejected along similar rationale.

As to dependent claims 22-24,these claims contain substantially similar limitations as dependent claims 11, 27, and 28; therefore they are rejected along similar rationale.

11.   **Claims 40, 41, 43, 47, 48, and50 are rejected under 35 U.S.C. 103(a) as being unpatentable over '672 in further view of '260.**

As to dependent claim 47, "locking the door" is shown in '672 col. 2, lines 2-3; the following is not taught in '672:

"wherein processing in the second step comprises the fifth step of, when the fingerprint authentication token is inserted into the main body in storing the article in the main body" however '260 teaches "A slot in the housing receives a removable smart card that includes a memory" in col. 2, lines 54-59;

"generating a password, storing the password in the storage means, transmitting the password to the fingerprint authentication token, and causing the fingerprint authentication token to store the password, and the sixth step of unlocking the door when a password based on matching between a registered fingerprint image and the fingerprint image detected by the sensor and output from the fingerprint authentication token is received in taking out the article stored in the main body, and the received password matches the password in the storage means" is however '260 teaches "Other steps include generating, at the host facility, a random number signal representing a random number in response to the ID code signal only if the ID code signal is representative of the ID code of the

device controlled by one of the registered persons" (note the "password" is interpreted to have

the same meaning as the "random number") in col. 3, lines 29-65.

It would have been obvious to one of ordinary skill in the art at the time of the invention

to modify the teachings of '672 a biometrical authentication method to include a means to

exchange passwords as taught in '260. One in the art would have been motivated to perform

such a modification because a method is needed to combine access codes used in the past with

biometric identification as indicated by '260 in order to protect the biometric information and

scol. 1, lines 17-43 "Each of these security systems can be operated by any person who is in

possession of the fixed code ... Therefore, each of these systems is inherently insecure ... it there

is a match, the requesting person is allowed entry or access to the host facility ... However, if the

set of authorized person is large, such a system would require a huge database to store the

fingerprint images ... and the identification process would become slower".

As to dependent claim 48, "wherein processing in the second step comprises the seventh

step of, when a password based on matching between a registered fingerprint image and the

fingerprint image detected by the sensor and output from the fingerprint authentication

token is received in storing the article in the main body, locking the door, and storing the

received password in the storage means, and the eighth step of unlocking the door when the

password based on matching between the registered fingerprint image and the fingerprint

image detected by the sensor and output from the fingerprint authentication token is received

in taking out the article stored in the main body, and the received password matches the

password in the storage means" is taught in '260 col. 3, lines 29-65.

As to dependent claim 50, **"wherein the method further comprises the 13th step of checking**

coins of predetermined amount, which are put in by the user in storing the article, and

processing in the first step comprises the 14th step of locking the door when that the coins of

the predetermined amount are put in is checked on the basis of processing in the 13th step"

is disclosed in 672 col. 18, lines 4-9.

As to dependent claims 40, 41, and 43, these claims contain substantially similar subject matter as

claims 47, 48, and 50; therefore they are rejected along similar rationale.

12. **Claims 7 and 19,** are rejected under 35 U.S.C. 103(a) as being unpatentable over '260 in

further view of '338 in further view of '260.

As to dependent claim 7, the following is not taught in the combination of '260 and '338:

"wherein said battery comprises a secondary battery charged by power supply from the

use device when said authentication token is connected to the use device" however '260 teaches

"Referring now to FIGS. 4A-4D, one embodiment of a PID 6B, which includes all the features also shown

in FIG. 1, includes a housing 44 similar in size to a personal pager or a small cellular telephone" in col. 8,

lines 14-40 it is obvious that a PID which is similar to a cellular phone would include rechargable batteries.

It would have been obvious to one of ordinary skill in the art at the time of the invention to

modify the teachings of '260 and '338 a portable personal identification system utilizing

biometrics that stores passwords in the personal devices to include a means to re-charge the

personal devices. One in the art would have been motivated to perform such a modification

because as indicated by '260 the PID is similar in size to a cellular phone (see '260 col. ever,

even in the individual authentication system using the IC card, if both the IC card (a physical

object) and the password (individual knowledge) are stolen, the safety is not secured ... an

object of the present invention is to provide an individual authentication system by which the

data processing device which needs individual authentication can be used and managed with

higher security".

As to dependent claim 19, this claim contains substantially similar subject matter as claim 7; therefore it is rejected

along similar rationale.

13.   **Claims** 42 and 49, are rejected under 35 U.S.C. 103(a) as being unpatentable over '672 in

further view of '260 in further view of '672.

As to dependent claim 49, **"wherein the storage further comprises a plurality of storage**

sections capable of independently storing articles and having corresponding doors" is

shown in '260 col. 12 line 63 through col. 13, line 11;

"in the ninth step is designated, and the fingerprint authentication token is inserted

into the main body" is shown in '260 col. 2, lines 54-59;

" locking the door," is disclosed in '672 col. 2, lines 2-3;

"generating a password, storing the password and the door number in the storage

means, transmitting the password and the door number to the fingerprint authentication

token, and causing the fingerprint authentication token to store the password and the door

number" is taught in '260 in col. 3, lines 29-65;

"and a password based on matching between a registered fingerprint image and the

fingerprint image detected by the sensor and output from the fingerprint authentication

token is received, and the received password matches the password in the storage means" is

shown in '672 col. 18, lines 17-33;

the following is not taught in the combination of '872 and '260:

"and processing in the second step comprises the ninth step of, when a corresponding door is closed in storing an article in a storage section, displaying a number of the door" and **" the 10th step of, when the door number displayed on the basis of processing"** and **"when the door number displayed on the basis of processing in the 11th step is designated"** and **"the 11th step of, when the fingerprint is authentication token is inserted into the main body in taking out the article stored in the storage section, displaying the door number stored in the fingerprint authentication token, and the 12th step of unlocking the door"** and however '672 teaches the in col. 2, lines 2-3 that the lock equipment has a mechanism to lock or unlock the object that is secured; '672 teaches in col. 10, lines 12-29 how the invention can be used on a trunk allowing the authorized person to lock and un-lock the trunk by the correct placement of their authorized fingerprint; 672 teaches in col. 11, line 63 through col. 12, line 13 how the system has an LED for displaying messages in combination with the logic received from the locking mechanism and biometric inputs, it would be obvious to incorporate the ability for an LED to display a room number. This feature is similar to the other example provided where a user can determine which locker they utilized in the coin operated locker by using their fingerprint and watch the for a flashing LED see col. 18, lines 17-23.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '672 and '260 a biometrical authentication method to include a means to display room numbers. One in the art would have been motivated to perform such a modification because a display is needed to show status information about the locking

mechanism as indicated by '672 in case someone forgot what locker they used see col. 18,
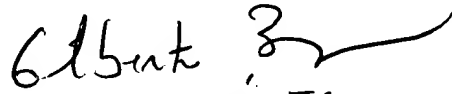
lines 9-50.

Conclusion

14.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Ellen C Tran whose telephone number is

(571) 272-3842. The examiner can normally be reached from 6:00 am to 2:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization

where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application

Information Retrieval (PAIR) system. Status information for published applications may be

obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the

Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197

(toll-free).

Ellen. Tran
Patent Examiner
Technology Center 2134
3 March 2006

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100